Дисциплина
«Методы защиты информации»

Рекомендуемая литература

1. Алфёров А. П. Основы криптографии: учеб. пособие / А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин. – М.: Гелиос АРВ, 2005. – 480 с.
2. Бабаш А. В. Актуальные вопросы защиты информации: монография / А. В. Бабаш, Е. К. Баранова. – М.: РИОР: ИНФРА-М, 2017. – 111 с.
   https://doi.org/10.12737/monography_58dbc380aa3a4.
3. Бабаш А. В. Криптографические методы защиты информации: учебник / А. В. Бабаш, Е. К. Баранова. – М.: КНОРУС, 2016. – 190 с.
4. Баранова Е. К. Моделирование системы защиты информации. Практикум: учеб. пособие / Е. К. Баранова, А. В. Бабаш. – М.: РИОР: ИНФРА-М, 2018. – 224 с. [Электронный ресурс; Режим доступа
   http: //www.znanium.com]. – DOI: https://doi.org/10.12737/18877.
5. Баранова Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. – М.: РИОР: ИНФРА-М, 2017. – 322 с. ww.dx.doi.org/10.12737/11380.
6. Маховенко Е. Б. Теоретико-числовые методы в криптографии: учеб. пособие / Е. Б. Маховенко. – М.: Гелиос АРВ, 2006. – 320 с.

Рекомендуемая литература

7. Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.
8. Нечаев В. И. Элементы криптографии (основы теории защиты информации): учеб. пособие / под ред. В. А. Садовничего. – М.: Высш. шк., 1999. – 109 с.
9. Рябко Б. Я. Криптографические методы защиты информации: учеб. пособие / Б. Я. Рябко, А. Н. Фионов. – М.: Издательство «Горячая линия-Телеком», 2012. – 229 с.
10. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2006. – 528 с.
11. Фомичёв В. М. Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты: учебник / В. М. Фомичёв, Д. А. Мельников. – М.: Издательство Юрайт, 2016. – 209 с.
12. Фомичёв В. М. Криптографические методы защиты информации. В 2 ч. Ч. 2. Системные и прикладные аспекты: учебник / В. М. Фомичёв, Д. А. Мельников. – М.: Издательство Юрайт, 2017. – 245 с.
13. biblio-online.ru (Электронно-библиотечная система).
14. znanium.com (Электронно-библиотечная система).
15. http: //e.lanbook.com (Электронные версии книг).

Лекция 1. **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ**

План

1. Проблемы защиты информации.
2. Угроза безопасности информации.
3. Классификация угроз:
   - 3.1. Угрозы доступности информации.
   - 3.2. Угрозы целостности информации.
   - 3.3. Угрозы конфиденциальности информации.

1. Проблемы защиты информации

Информационная безопасность является одной из главных проблем, с которой сталкивается современное общество. Причиной её обострения является широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

Решение проблемы информационной безопасности связано с гарантированным обеспечением трёх её главных составляющих: **доступности, целостности и конфиденциальности** информации.

- *неавторизованный доступ к информации;*
- *неавторизованное изменение информации;*
- *неавторизованный доступ к сетям и сервисам;*
- *другие сетевые атаки, например, повтор перехваченных ранее транзакций и атаки типа «отказ в обслуживании».*

Криптография

Вопросы сохранения и передачи конфиденциальной информации решает **криптография – наука о методах преобразования информации в целях её защиты от незаконных пользователей**.

2. Угроза безопасности информации

Под **угрозой безопасности информации** понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию.

Целью защиты информации является предотвращение нанесения ущерба пользователю, владельцу, собственнику информации.

Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо проводить защиту в соответствии с поставленными целями.

Под **эффективностью защиты информации** понимается степень соответствия результатов защиты поставленной цели.

Свойства информации

- **Доступность** – возможность за приемлемое время выполнить ту или иную операцию над данными или получить нужную информацию
- **Целостность** – актуальность и непротиворечивость хранимой информации
- **Конфиденциальность** – защищённость от несанкционированного доступа

Защита информации

Информационную безопасность, построенную на обеспечении доступности, целостности и конфиденциальности информации, называют ***моделью CIA*** (от англ. *Confidentiality* – конфиденциальность, *Integrity* – целостность, *Availability* – доступность).

Определение 1. ***Под защитой информации понимают комплекс мер, направленных на обеспечение информационной безопасности.***

Определение 2. ***Под угрозой информационной безопасности понимают действие или событие, приводящее к нарушению достоверности, целостности или конфиденциальности хранимой, обрабатываемой или передаваемой информации.***

Рассмотрим понятия, которые часто используются при анализе безопасности информационных систем

– **атака** – попытка реализации угрозы

– **злоумышленник** – лицо, осуществляющее атаку

– **источник угрозы** – потенциальный злоумышленник

– **окно опасности** – промежуток времени с момента появления возможности использовать слабое место в защите до момента ликвидации этого слабого места

3. Классификация угроз

1) *угрозы доступности информации*
2) *угрозы целостности информации*
3) *угрозы конфиденциальности информации*

Классификация угроз по их характеру

Случайные и **преднамеренные угрозы**

Случайные угрозы возникают независимо от воли и желания людей, хотя последние могут являться источниками этих угроз.

Преднамеренные угрозы создаются людьми, в результате их целенаправленных действий.

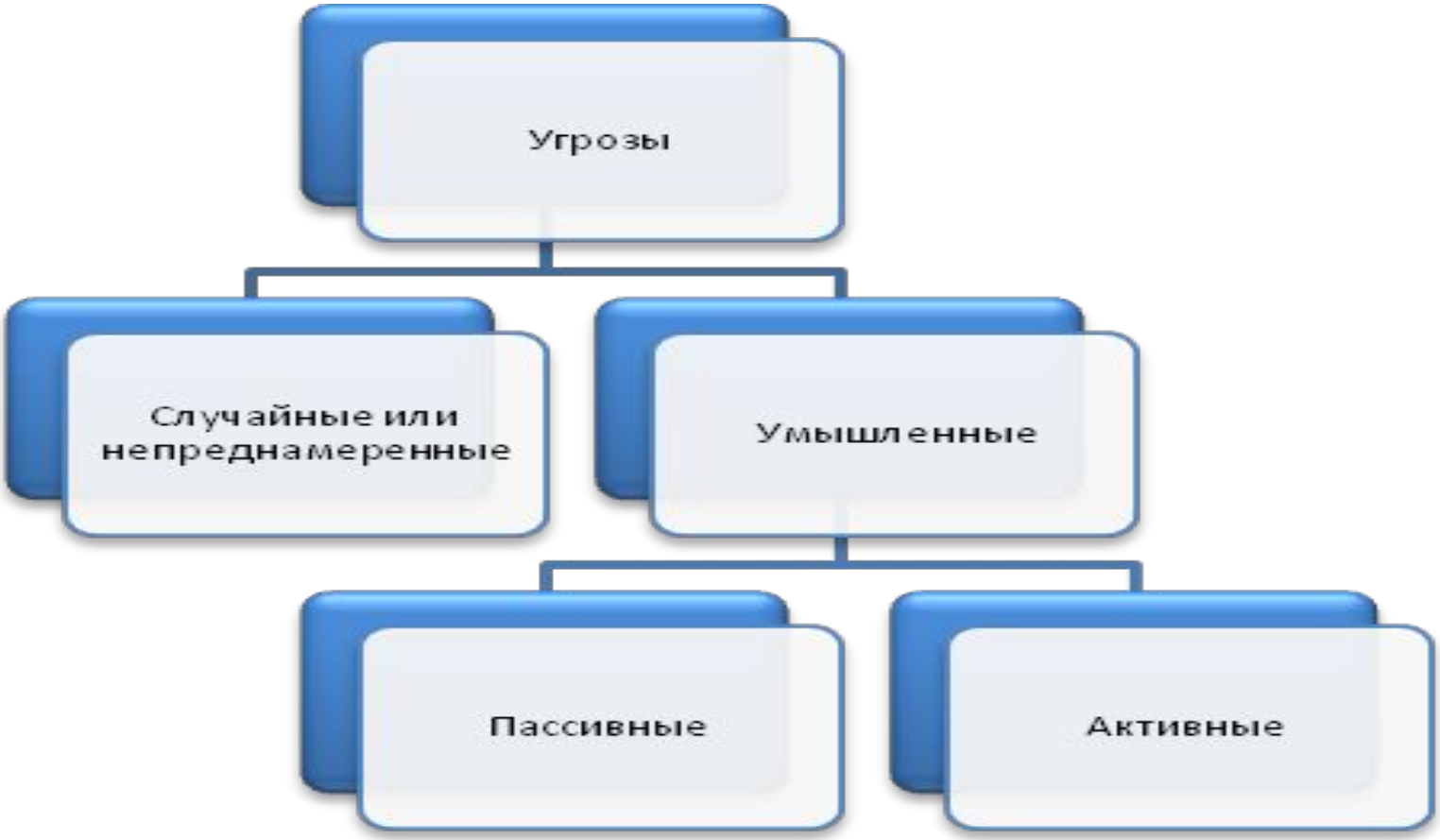
Классификация угроз по источнику

- **Природные угрозы** являются случайными и связаны, прежде всего, с прямым физическим воздействием на компьютерную систему или системы её жизнеобеспечения.
- **Технические угрозы** вызваны неполадками компьютеров, средств связи и другого оборудования, а также проблемами в работе программного обеспечения. К техническим угрозам относятся и неполадки в системах жизнеобеспечения зданий, тепло-, водо-, электроснабжения и т.д.

Угрозы, созданные людьми

- **угрозы со стороны людей, непосредственно работающих с информационной системой** (обслуживающего персонала, операторов, программистов, администраторов, управленческого персонала и т.д.);
- **угрозы, вызванные внешними злоумышленниками** (хакерами, разработчиками и распространителями компьютерных вирусов и т.д.).

Виды угроз


Угрозы
Случайные или непреднамеренные
Умышленные
Пассивные
Активные

Источники случайных или непреднамеренных угроз:

- ошибки в программном обеспечении;
- выходы из строя аппаратных средств;
- неправильные действия пользователей.

Умышленные угрозы преследуют цель нанесения ущерба пользователям компьютерных систем

- ***Пассивные угрозы*** – направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование компьютерной системы.
- ***Активные угрозы*** – имеют целью нарушение нормального процесса функционирования компьютерной системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

Основные угрозы безопасности информации

- раскрытие конфиденциальности информации (несанкционированный доступ к базам данных, прослушивание каналов и т. д.);
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией и т.д.

3.1. Угрозы доступности информации

- ***отказы пользователей*** (системных аналитиков, системных и прикладных программистов, системных администраторов, конечных пользователей);
- ***внутренние отказы информационной системы;***
- ***внешние источники возможного нарушения доступа к данным***

Средства защиты доступности информации

1. Правильная организация труда.
2. Подготовка и подбор кадров.
3. Тщательная и полная разработка информационной системы, в том числе удовлетворяющая работников пользовательского интерфейса.
4. Тщательное тестирование информационной системы, в том числе на предмет критических ситуаций (при большой нагрузке, больших объёмах обрабатываемой информации и т.п.), и на предмет ввода заведомо неправильной информации.
5. Резервное копирование данных.
6. Наличие резервного оборудования, помещений, подготовка персонала к действию на случай нештатных ситуаций.
7. Средства защиты каналов связи, например, от воздействия внешнего электромагнитного излучения.
8. Комплекс мер по защите от сетевых атак, вирусных и других вредоносных программ.
9. Межсетевое экранирование. Экранирование – это способ фильтрации потоков информации между двумя сетями (или двумя информационными системами).
10. Протоколирование (запись в журнал) всех действий, которые совершают пользователи.

3.2. Угрозы целостности информации

Основными средствами защиты целостности информации в ИС являются:

- транзакционные механизмы, позволяющие восстановить целостность данных в случае незначительных сбоев;
- контроль ввода данных;
- использование средств защиты целостности СУБД;
- резервное копирование данных;
- периодическое тестирование системы на предмет нарушения целостности.

3.3. Угрозы конфиденциальности информации

Определение 3. ***Конфиденциальная информация - информация, на которую распространяются правила разграничения доступа.***

Определение 4. ***Под правилами разграничения доступа понимают совокупность положений, регламентирующих права доступа лиц и процессов к единицам информации.***

Выделяют два вида конфиденциальной информации: ***служебную*** и ***предметную***. К служебной информации, в частности, относятся имена и пароли пользователей. Зная служебную информацию, можно получить доступ к предметной информации.

Несанкционированный доступ к информации возможен:

– при отсутствии системы разграничения доступа;

– при ошибках в системе разграничения доступа;

– при сбое/отказе программного или аппаратного обеспечения;

– при ошибочных действиях пользователей или обслуживающего персонала;

– при фальсификации полномочий;

– при использовании специальной аппаратуры и ПО.

Возможные пути несанкционированного доступа к информации:

- перехват электронных излучений;
- применение подслушивающих устройств;
- хищение носителей информации и документальных отходов;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- использование программных ловушек;
- незаконное подключение к аппаратуре и линиям связи;
- внедрение и использование компьютерных вирусов и т. д.